

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
ROANOKE DIVISION

IN THE MATTER OF THE SEARCH OF:
**TONY'S DELI MART, 605 11TH STREET
NW, ROANOKE, VA 24017**

Case No. 7:20mj95

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Melissa J. McAlister, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as Tony's Deli Mart, 605 11th Street, N.W., Roanoke, VA 24017, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a U.S. Postal Inspector with the U.S. Postal Inspection Service (USPIS), and have been since July 2014. My responsibilities include the investigation of crimes involving the United States Postal Service and crimes furthered through the use of the United States Postal Service. This includes, but is not limited to, the investigation of the theft of U.S. mail, fraudulent use of such stolen mail matter, robberies, burglaries, and assaults. I have received formal training in conducting these types of investigations as well as identifying and securing evidence related to such investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth herein come from my own investigation, observations, training and experience, and from information obtained from other law enforcement officers and witnesses.

4. On July 16, 2020, I asked the owner of Tony's Deli Mart, Amjad Shareef Ibrahim, if he would voluntarily provide me with the surveillance video footage requested herein. Mr. Ibrahim has not responded to my request and my efforts to communicate with him have proven unsuccessful. Therefore, I do not believe he will provide the evidence sought without a lawful process being served upon him. The warrant I am applying for today will allow for the prompt seizure of the evidence discussed below.

PROBABLE CAUSE

5. On July 14, 2020, a female customer came into the Melrose Branch Post Office (Roanoke, Virginia) at approximately 12:15 P.M. to purchase a United States Postal Service (USPS) money order. A disagreement occurred between the customer, who was wearing a mask, and an USPS employee regarding the amount of money needed to complete the transaction. A second USPS employee, identified as F.M., intervened to resolve the issue. As F.M. was speaking to the customer, F.M. alleges that she was head-butted by the customer. Your affiant notes that none of the witnesses observed the head-butt and there is no video surveillance of the altercation. Your affiant is presently investigating this matter as a potential violation of Title 18, United States Code, § 111.

6. To date, the investigation has revealed certain information relating to the suspect's identity. During the incident, a different customer called the suspect customer "Mona."

While none of the witnesses interviewed knew, or provided, “Mona’s” last name, law enforcement was able to obtain a physical description of “Mona.” USPIS also determined that “Mona” worked at or frequented Tony’s Deli Mart. Tony’s Deli Mart is a convenience store located in Roanoke, Virginia, within the Western District of Virginia, and has a physical address of 605 11th Street N.W., Roanoke, Va. 24017. F.M. stated during her interview that “Mona” told F.M. not to come around “her store.” F.M. stated she does not regularly deliver mail and the last time she delivered any mail to a store was approximately sometime during the first week of July 2020. F.M. indicated she delivered mail to Tony’s Deli Mart during that period of time.

7. Continuing on July 14, 2020, USPIS spoke to an employee at Tony’s Deli Mart who was able to confirm that a “Mona” does frequent the store, but is not employed there. The physical description of the “Mona” the store employee described matched the physical description of the “Mona” provided by witnesses to the incident. This employee advised that Mona had been inside Tony’s Deli Mart on July 14, 2020, at approximately 12:00 P.M. According to a “directions” search using Google, Tony’s Deli-Mart is just over 2 miles away from the Melrose Post Office.

8. The store employee was also able to confirm the store’s video surveillance cameras worked. Unfortunately, he/she could not access the camera system and did not know how long the video was kept. Your affiant gave the store employee her business card and asked the employee to pass along your affiant’s contact information to the store owner.

9. USPIS made inquiries via CLEAR, an electronic database that has proven reliable in previous investigations in determining the legitimacy of name, address, and phone number

information, to conduct searches for information related to Tony's Deli Mart. USPIS was able to locate a name and phone number for the owner of Tony's Deli Mart and confirmed the name with postal records.

10. On or about July 15, 2020, Postal Inspector S. McCafferty was able to get in touch with the owner of Tony's Deli Mart. The owner confirmed "Mona" did not work at Tony's Deli Mart. The owner stated he would review the video footage and contact Inspector McCafferty once he did so. Inspector McCafferty never received a return phone call. On or about July 16, 2020, your affiant attempted to contact the owner of Tony's Deli Mart, but met with negative results.

11. At this point in the investigation, USPIS only has a physical description of the suspect customer and a first name. Therefore, based upon the foregoing, your affiant submits that probable cause exists to believe that the identity of "Mona" can be determined by reviewing video footage preserved on the surveillance system installed at Tony's Deli Mart. Your affiant seeks to review the footage from July 6, 2020 through July 14, 2020 as these encompass the dates F.M. may have been inside the store and are also dates in which it is reasonable to believe that "Mona," a frequent customer, would have also been in the store, including the date the incident occurred.

TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, a DVR, hard drives, or other storage media associated with, or connected to, any security surveillance system on the PREMISES on which electronic data and images may be stored. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

14. *Probable cause.* I submit that if a computer, DVR security system, hard drive, or other storage medium associated with any security surveillance system is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. The owner of the PREMISES confirmed that there is a video surveillance system in place that has playback capability.
- b. Based on my knowledge, training and experience, video surveillance is kept on a storage device from anywhere between 14 days to 60 days. This range is based on the type of video surveillance equipment, the type of storage device, the available

memory on the storage device, and the settings selected on the video surveillance software.

15. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate electronically stored videos, images, or files that might serve as evidence of identification in an effort to discover the perpetrator of the above-described alleged assault on a postal employee in violation of Title 18, United States Code, § 111, Assaulting, resisting, or impeding certain officers or employees. Based upon the foregoing, there is probable cause to believe that this forensic electronic evidence will be on a computer, DVR, hard drive, or other storage media associated with, or connected to, the business's security system.

16. *Necessity of seizing or copying entire computers, DVR, hard drives, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As explained above, because the warrant calls for the seizure of forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain such evidence.

Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and may be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and, if necessary, would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to

computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

18. Tony's Deli Mart is a functioning company that conducts legitimate business. The seizure of the Company's computers, DVR, hard drives, or other storage media associated with their security surveillance system may limit the Company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, DVR, hard drives, or other storage media it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

*****THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK*****